

- Filename: eccouncil-ceh31250-v11-4-7-1-smtp-enumeration.md
 - Show Name: CEHV11 (312-50)
 - Topic Name: Recon Techniques - Enumeration
 - Episode Name: SMTP Enumeration
- =====

SMTP Enumeration

Objectives:

- Use common SMTP commands and tools to enumerate valid user accounts
 - Enumerate FTP for possible sensitive and/or actionable information
-

- SMTP is used to send email, so how can that be leveraged for enumeration purposes?
 - Users
 - email addresses
- How?
 - SMTP server commands
 - VRFY
 - EXPN
 - RCPT TO
- How to we make use of these commands for enumeration?
 - Login directly
 - netcat
 - Telnet
 - smtp-user-enum
 - -U/-u User list / single user
 - -t Target mail server (IP)
 - -M Mode (VRFY,EXPN,RCPT TO)
- What about FTP?
 - Anonymous login?
 - If yes, is there any sensitive info that can be viewed?
 - Can anonymous upload?
 - Brute-Force login
 - Version info
 - Known vulnerabilities?